

Lab 08 Template – Ethan Roepke

Some questions require multiple parts to be answered, be sure to discuss them in full.

Part 01:

1. Screenshot of the output from `openssl rsa -text -in <netid>_private_key.pem` (10 points)

```
Private-Key: (2048 bit, 2 primes)
modulus:
00:99:3f:64:0e:6d:b8:e5:bd:b2:1f:96:d2:1d:0b:
d5:c7:43:17:a4:57:b3:60:7c:91:b3:0b:7e:e7:70:
1e:c6:8b:81:7a:d3:12:dc:92:7c:e8:cc:11:9f:31:
c0:96:60:9a:2f:62:33:ab:7e:c7:91:0c:65:b2:be:
9e:e8:67:fc:cf:e4:e0:35:74:2a:a0:63:a3:c3:d2:
33:0c:f7:89:87:7b:4e:d8:c4:5e:2f:f6:65:b3:ba:
87:59:22:e2:e3:55:a4:f1:ac:fa:a0:96:1b:34:4b:
5f:2c:1a:a3:77:50:7c:97:f9:a2:1c:1e:57:1f:c1:
55:b9:f6:1a:ab:86:f5:d7:28:93:35:56:89:06:53:
dc:2d:94:68:4f:c1:2e:70:7a:df:ea:9e:60:9f:d1:
50:7d:3b:18:93:1d:ed:82:14:7a:8c:f5:e4:ef:16:
64:fa:f0:f6:cc:43:00:ff:c4:01:6f:c9:ce:57:13:
77:45:d5:a0:fe:b0:69:04:d0:67:ad:ce:b5:bf:7b:
5c:ae:c3:d0:53:5a:2b:fa:ab:1c:9e:35:f3:e3:bf:
38:f4:15:59:8a:66:e5:79:a2:02:58:fb:80:a2:89:
87:19:07:c2:a4:67:02:d7:bc:cd:86:8c:4e:a3:25:
9e:2d:3b:cc:58:47:9f:aa:e6:91:63:96:c6:81:43:
41:13
publicExponent: 65537 (0x10001)
privateExponent:
09:ac:8d:9f:db:8d:55:18:04:86:95:67:ee:2d:7a:
3a:79:2d:b6:5e:1c:14:bf:c8:60:89:b0:19:2c:1a:
c5:40:74:f0:e9:f4:79:25:d8:7c:c7:65:1e:87:93:
37:a1:d8:63:09:ef:f9:15:cc:55:a0:52:b8:e8:34:
3b:49:e7:82:93:a2:81:74:33:e1:3e:69:01:4a:75:
f7:b2:71:d2:fb:a8:0c:47:10:06:80:39:bd:a3:5f:
a7:f3:22:b1:d2:9f:64:b4:8b:54:a1:00:9f:c7:eb:
6c:6b:0b:38:f8:69:77:65:6a:da:f6:f7:12:24:1d:
b7:91:d6:38:99:35:99:76:46:53:f6:3f:9a:36:11:
fa:b0:f1:a0:22:c7:31:f0:4b:5d:08:a2:93:63:e4:
c3:81:6e:cd:88:83:f5:6a:cf:0a:2a:a1:b1:cd:83:
1a:34:20:94:d1:08:a2:3f:b7:ce:a9:e0:e4:81:2e:
47:64:26:d5:ab:b0:a7:76:be:cb:54:6a:38:48:04:
93:6c:b6:59:31:0e:a4:3e:f5:aa:54:67:d0:a2:63:
c9:f5:69:c0:e8:b1:92:05:1d:4e:68:80:51:4c:fd:
28:7b:21:0e:cf:24:52:b6:bf:03:f4:9b:0e:77:7d:
7e:da:bb:f9:46:17:1b:15:1a:e4:04:a8:03:59:b9:
01
prime1:
00:d5:1d:0d:e6:53:f3:61:18:16:82:7f:8f:99:49:
d6:ed:4d:b4:83:93:38:1d:cc:fa:b7:2d:28:0b:f8:
b0:85:87:26:d0:50:03:cb:24:66:ba:37:d7:24:11:
a3:41:ab:e6:a0:8d:78:9d:f0:60:be:7e:71:b0:a1:
f4:05:9e:51:6e:93:cd:aa:ff:97:cb:2b:6c:f2:71:
43:bd:b0:d4:a3:29:d1:1d:14:61:7a:53:02:2d:19:
a5:9c:01:0c:58:e6:36:c3:db:a8:2f:cb:d8:f1:b6:
b5:8d:2e:36:2f:5d:7c:1c:60:d8:5b:ac:14:57:43:
c9:36:bf:e0:ea:43:f7:f3:b5
prime2:
00:b8:16:3b:8b:54:d1:b9:69:0a:92:70:bc:05:04:
a8:13:2a:cf:4c:2e:6c:fd:55:59:45:99:6a:30:de:
78:54:c0:0c:4b:b8:27:ef:eb:73:14:b4:fe:44:1d:
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQFAASCBKggwggSkAgEAAQIBAQZP2Q0bbjLvbIf
ltIdC9XhQxekV7NgfJGzC37ncB7G14F68xLcnzozBGFmcWY3ovYjOrfseR0QW
vp7oZ/zPSOA1dCqyGP0BjMM94mHe07Yx4v9mKzuodZ1uLjVatXrPagLhs0518s
GqN3UHyX+aIClCfWm59ghrhwXXXKJ1VokGU9wtLGHpW5Swet7/qnnCF0VB90xIT
HeZCFHq9eTvFnt68PB0Qw0/xAFvycSXE3dF1a0+sGKEGetzrW/e1yuv9BTWlv6
qxynFPjvzj0FVmkZuV5ogJY+4CLLYCZB8KkZuLXN2GJ6jJ24t08XYR5+q5pfj
LsaBQ0ETAgmBAEACggEACayhnsuNVrgEhpVn7160nn9N14eFL/IYImGSwaxUAK
sonheSXYPdLHoeTH6YfYmW+RXWn8Suoq00mngp0lgQ0z245PaUp1973x0vuo
DEc0Ba0SvaNfP/MLsdKfZLSLVKEan8FrbGdLORhp2Lqzv69E1Qdt5HMOJk1nXZG
U/Y/njYR+rDxoLHMfBLXQ1Lk2Pkw4FuzYLD9WrcPQhsc2DQJ0gINEIoj+3zng
51Eur201auwp3a+y1Rq0EgEk2y2WTEOpD71qLrN8K3jyFvPw0LxkgldmIAUuz9
Khsh0SbKlraJA/5b0nd9ftq7+UYXGxUeS0A5o1n5AQW8Q0W0H3mJ/nhGBCaF+z
SdbtTb5DKzgdzPq3L5gl+LCFhybQUAPL3Ga6N9ckEaBq+agjX1d8GC+fnGwofQF
nLFuk82a/5FLK2zyU09sNSJKdeDFG6UwItGAmcAqY5jib26gvy9jxtrWNLjYv
XXwYnHbrBRXQ8k2v+DqQ/fztQKBgQC4fJulVNG5aQq5cLwFBKgtKs9MLnz9VVlF
Mkw03nhUwAxlucFv63MUTPSEHft+qcJAanSoOE/L+HOCtC0KcP+HJ7LjQcHJCKg
nUBtoKofvKAgvL2zr+HnBcYX0XZ0TpgfPCD855FkLceJra5wJXmVc4DgPYECMNL
yHkR3Jupw8DgftfmgBw0DORre/K5GppKAmfJAT5hy6cdpddFOYQvJKSR0heCqP
5AqLERZ0B3qPv52Ar3KcrCAKMDp3P50q0LwE16gnteeTEphakn8a8gh3aBc
z0Guzt8ZDEda5ZF1NGSXKjykF4B89r8s9L1CncBmCAT5TXYTQ1DCNsJCRAoGBAIO2
T3ZNet1RXeIXTT/7D8ACwL2EnJ0IX15fJU3H75rb6jBHLDDKZ8M6Fm9Q0IBZIAwM
4EArgLSz1J030eU+0Z55/1M4GL8eBZUs8Z8+pegEXhUYX4AZ5ungGrqvQvYCT1
HEWMLsShyMTA4R3gVCPmhxnR520z+MayfIpaTL/JAoGBAI/N0nKTPLOkav0SLaIP
vv3x3p2Hvr203j4T38HeRALXenzJHKggyYLPOLjgfnB2LUpz5Rj1jXKTEjW+RCEN
gtIznkeuTn2PqGQRH0EgLT2A16oXTD01Z/3wyngZL1La305Hw/eWf6+ep20E9YON
whJVF29+CHS6/Ee91K0ewDw2
-----END PRIVATE KEY-----
```

2. Comparison of the same/different values observed across the extra generated keys. (15 points, 5 points each question)

```
Private-Key: (2048 bit, 2 primes)
modulus:
00:a4:b4:99:bd:69:94:10:67:08:f8:a6:95:25:4b:
50:66:2e:11:a0:0b:7f:a6:39:94:d7:a3:ea:ec:cb:
4b:ce:c1:dc:e9:52:f1:fc:cd:79:23:a1:7a:4c:0e:
c4:a4:7d:b1:ef:37:8b:3b:f1:02:16:dc:5c:cf:5d:
a1:d7:d2:10:82:f9:0d:94:80:c0:17:4e:a8:fd:b2:
72:9f:e6:bf:9c:83:f6:f4:73:07:7a:2e:bc:09:52:
a8:37:3f:81:7f:3a:3d:5d:28:64:99:ac:3f:53:22:
65:7b:7f:7d:75:7d:c7:47:06:a8:88:5e:21:06:78:
fa:71:92:21:09:1a:e4:59:44:46:b5:a7:9c:31:91:
1b:cb:40:c3:94:25:44:77:6f:d6:6f:8b:71:2a:fc:
d5:ce:e1:62:0a:56:22:61:af:e8:6d:7d:68:cc:3a:
d2:ed:51:7b:6a:3a:6b:75:e0:c3:28:a7:20:1a:52:
c4:b9:de:c5:b5:13:b3:63:0d:a4:ad:45:9d:1f:df:
30:ce:47:f6:3d:62:1c:55:c4:5b:11:92:40:f1:92:
42:18:a9:c1:8f:9a:2e:77:54:11:10:f7:c6:c1:cc:
96:f9:da:82:19:60:09:2e:34:9f:ff:c7:1f:f4:18:
3d:ad:d6:c1:5e:01:55:94:56:39:bd:05:52:6d:10:
70:1d
publicExponent: 65537 (0x10001)
privateExponent:
04:0e:8f:bf:de:df:1f:05:4e:af:03:39:66:bd:03:
6a:b4:e5:49:b6:26:c3:83:25:13:a7:ad:b4:6d:f0:
7c:d4:01:1b:3d:28:09:3c:ad:68:cf:84:29:e5:ee:
3b:1b:0e:7b:0b:30:4d:06:6a:f1:01:b5:06:84:0d:
a5:39:7f:1f:1e:bf:d3:21:d5:b9:6d:3e:53:db:66:
9f:e2:28:e3:93:cb:8c:2b:5e:2a:88:06:a9:2b:28:
4a:16:16:1c:3a:6d:c3:0b:e8:e8:71:19:f1:34:06:
70:63:8c:45:4d:d7:42:6e:5b:4d:da:95:b1:29:5f:
2f:d7:73:d9:5b:0d:76:93:62:0f:2a:29:1a:ea:4a:
2f:0b:88:6d:bd:b2:1e:37:de:f0:97:08:c4:17:46:
be:ae:29:59:db:ac:81:28:58:01:c7:6e:c4:ea:4f:
28:eb:85:81:f2:82:15:9d:97:be:ca:a1:f4:09:11:
a1:2f:d1:39:65:88:9c:c6:bd:d0:86:f0:41:01:32:
1a:da:7a:7e:77:79:d9:d6:72:83:59:6a:67:7f:bc:
45:58:6e:02:1c:5f:01:97:ee:f4:c6:b3:7e:3c:91:
c6:e7:bb:18:93:24:41:ba:ce:ea:58:aa:f5:8d:b4:
e1:52:21:ad:b0:ae:d4:39:bf:71:29:26:1d:9d:1b:
69
prime1:
00:dc:aa:13:d0:e4:57:58:a6:6b:d3:f7:e9:ce:3f:
ff:69:69:12:cb:d4:30:60:7d:b4:ae:bd:3e:52:73:
12:4d:47:f9:a1:a3:46:f8:93:65:04:90:48:6c:
9c:65:62:ff:f9:26:50:4e:aa:59:e2:f5:d9:44:b9:
cc:a1:78:63:9c:fd:ce:23:d4:b1:48:f9:e2:6b:c0:
36:21:d0:59:ce:33:51:2d:4c:6b:2e:c1:8c:be:48:
ce:e7:e0:ba:18:55:43:08:3e:11:07:11:80:dd:d0:
32:fe:5c:03:db:d0:b5:6f:09:26:8a:06:62:9c:01:
53:83:73:40:43:0e:5e:82:35
prime2:
00:bf:14:8a:d4:af:9b:32:da:f9:93:35:9b:87:5b:
8f:2a:b3:c5:9f:92:06:3f:eb:6a:6c:f6:e5:8f:cf:
65:00:45:70:a9:17:93:21:05:0c:5c:a8:07:ef:b6:
a7:bb:95:24:fe:02:cb:5d:8e:d5:6c:35:5f:ef:d2:
36:ba:c0:0a:fd:90:a6:57:f0:7f:08:24:9e:5d:a1:
ff:3d:b0:15:a3:3e:b0:21:09:30:85:a2:bc:d1:48:
57:01:08:54:ca:cd:54:e7:81:c8:4a:7e:7f:4a:4f:
eb:e1:c3:8b:de:e2:75:2c:9a:23:f2:2b:83:f1:87:
d1:67:86:37:84:35:11:f3:49
exponent1:
00:c1:40:e2:a1:eb:98:e3:b6:bc:70:a3:8a:4c:6b:
98:10:85:49:44:e1:cc:8c:75:0b:2c:8d:e8:6a:e5:
04:7e:52:2e:b9:f4:f9:51:eb:5d:8a:f6:f8:35:b5:
89:32:f2:05:23:fa:fe:12:26:f7:19:e2:1e:2a:26:
5e:a4:7b:7f:22:1a:d5:d2:63:8f:f0:4d:88:92:bd:
7f:ab:15:81:d1:28:f8:4b:27:c6:26:e8:b3:8e:62:
cd:72:1e:4a:5c:cd:2f:2b:a4:cf:dc:d4:e3:7b:5f:
bf:89:2c:a4:e4:7a:60:ab:a1:e3:f2:b5:ac:de:db:
fa:7c:01:0f:a2:aa:8e:f2:91
exponent2:
45:fc:7c:2d:12:74:c1:d7:ba:79:d4:b4:b6:8b:2e:
90:f1:0f:7c:d6:bb:3b:46:3a:a0:d6:7d:96:82:dc:
49:9c:a5:7b:09:8b:76:18:a7:42:78:b9:0f:6f:d3:
46:28:c6:77:d3:06:31:aa:53:39:63:03:54:8f:a6:
44:18:7a:ee:0c:c1:20:8c:91:ba:a5:ce:eb:74:9e:
4c:35:e6:76:f8:4b:02:8e:9f:1b:13:54:1d:43:65:
ba:97:16:97:86:c4:02:57:62:c9:06:34:11:3f:dc:
a1:c0:41:c6:cd:23:25:c6:ff:4b:7f:ec:bf:d6:83:
38:6b:cc:81:bb:fe:6b:21
coefficient:
2b:59:96:9e:1a:74:b8:1a:86:ca:dd:b0:ca:3d:09:
ab:e0:49:90:2c:05:db:6e:3f:66:2b:07:f0:b4:b7:
33:0b:ca:54:1a:10:19:ff:5f:23:c4:4c:95:f3:2b:
eb:95:c2:75:fa:c0:eb:39:9a:d6:0e:2f:d2:af:a4:
2b:a9:f1:4d:fb:78:f6:ed:bf:31:7e:e2:af:ab:06:
b6:40:19:22:25:79:e5:3c:6d:6c:68:27:10:26:28:
6b:b1:79:2d:43:ef:dc:5a:e4:5f:33:6e:ef:6d:30:
c5:14:f5:fd:71:5b:fb:7b:87:9f:d5:8f:d8:86:9d:
bf:fd:1d:8a:f9:29:92:35
-----BEGIN PRIVATE KEY-----
MITEvQIBADNBgkqhkLc9w0BAQEFAASCBKcwpg5JAgEAAoIBAQCktJm9aZQZ2wJ4
ppULS1BmLhGgC3+mOZTXo+rsy0vOwdzpUvH8Zk-joxpHdsTkfBhVn4s78QIw3fzP
XaH0HCC+QZUgMAXtQj9snKF5r+cg/b0cdw6LrWJug3P4F/0j1dKGSZrD9T1m7f
f311fc9BqLIXLEGEppxkLEJGURZREa1pSwxKRVLQMOJUR3b9ZvL3Eq/N0x04WIK
VLJhr+htfWJm0TLtUXt0nt1dMopyAaUs535m1E7Nj0a5STR0f3zD0R/Y9YhXv
xFSRkdkkL1YqCPmLS3VBE998bZJb52oIZYAKuNj//xx/0G02t1sFeAVMUNjm9
BV0tEHADAgBAAECggEABAg6p97fHwJ0rW5Zr60arT1Sb4mwKLEgetG3wFVq8
Cz0oCTNkMwEKaXU0u0e7AwTYzQ8QC2BoNpTL1/hx6/BYHwJ0eU9tgn1o45PL
JctekogG45sg5hVh0p6kwv6Ez8TQCcCOMRU3XQcSBtdvS1FL9dz2VrQdpKt
DropeGupLwL1a92zHjfe87c1xbDvudphidugSHYAcduxOpK0uGfKCFZ2XvsgH
9AkRoS/ROwInMbb0Ibw0QEyGp6fnd52dzYp1qz3zBRVhuAhxFAZfu9Wazf3jR
xue7C3WkqBROGLlq9Y204VtHrQuuIDm/cSkw4Z6baQK8GdcqahPQ5fdywvT9+r0
P/9paRL1L08gfbSuvT5ScJNR/h0b7+Jm18Jb1b3xLV/5318oqln19dLEucyh
eGDC/c4j1f1e3rW0Yh0Fm0iETGsuYy+5M7n4L0vUUMPHHEYD08LxAPb
0LVVCSaK8McAVODcB8D016CQK8GqC/FtUr5y2mTN2uM48qs8Hfkgv/62ps
9uWPz2XpRXCP5MH8QxcqAfvtaeLST+Astd3tVnM/v0j6wAr9KkZX8H81J35d
ofB9s8WjPrahCTCFrZRSFbCFTK3FTngchKfn9Kt+vhWde4nUsnPyK4Pxb9fn
hjeENRHz5QK8G00B00K65j1trxo4pMa5g0HLE4cykD0ssJeh50R4UL659P1R
612Kvg1tYkyBglj+v45Jvc24h4qJl6ke38lGtXSY4/wTYt5vX+FYHRKPhL3BvM
6LD0Ys1YhKccz58rPh/c10N7X7+JLTKemCroePytaze2/p8A0+Iqo7YkQK8EX8
fC85dM4XunnUtlalLpdx3zWuztG0qDWFZaC3EncpXsJ3YpP034u09v08YoxnfT
BjGqUz1J315Ppk0Yeu4W5CkHbqLzUt0nkW15nb4SwK0nxTVb1DZbqXfpeGxAX3
YskANBE/3KHQcBNiYXG/0t/7L/WgzhzIG7/mshAoGAK1mnhp0uBqGyt2vyJ03
q+BjKcWf224/Z1sH8L3MwKvBoQGF9f18RmLfmr65XCdfRA6zma1n4vBq+kk6nx
Tft49u2/WX71r6sGtKAZ1LV55TxbGgnECYoa7F5LUPv3FrAXXZNU270wRt1/Xfb
+3uHn9WP2Iadv/0d1vkpkJU=
-----END PRIVATE KEY-----
(END)
```

a. Which values are constant?

The key length bit will stay constant since we are using 2048 bits. The RSA key identifier will stay constant as well

b. Which ones vary?

The public key and private key will vary after each new generation. The public key will vary as its mathematically linked to the private key and unique to each pair. The private key will vary because of the random generation for the key.

c. What do these values represent?

The public key is distributed to others and allows others to encrypts data with only the matching private key that can decrypt.

The private key is the secured key that is held with the user and used to decrypt data with public key.

The key fingerprint is used for quickly verifying kids without revealing the full key data.

3. Discussion of the differences between FTP and SFTP.

(15 points, 5 points each question)

- a. Why would you want one over the other?

SFTP offers a secure port for data transfer, while FTP transfers data not secured so in plaintext which is sustainable for attacks. SFTP will encrypt the data and authentication which will protect sensitive data while transferring data. I would want SFTP over FTP for security reasons.

- b. Why did we need to specify our private key?

We needed to specify our private key to authenticate securely without using just a password. The server will hold the public key and the user would hold the private key and when we specify our private key, only the authorized user with private key can access the server.

- c. What protection does this offer?

Having public/private key offers much more security not relying on passwords that are prone to brute force. Even an attacker knowing the public key, they cannot get the correct private key since the user has it with them at all times.

4. Screenshot of the five messages [netid]1.txt, [netid]2.txt, ... [netid]5.txt(10points)

```
cpre3310@cpre3310:~/homework/lab08/eroepke$ ls
cacert.pem eroepke1.txt eroepke2.txt eroepke3.txt eroepke4.txt eroepke5.txt lab08_public_key.pem sig.txt.sha256
cpre3310@cpre3310:~/homework/lab08/eroepke$ cp lab08_public_key.pem ..
cpre3310@cpre3310:~/homework/lab08/eroepke$ cp cacert.pem ..
cpre3310@cpre3310:~/homework/lab08/eroepke$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 eroepke1.txt 2>/dev/null
Verification failure
cpre3310@cpre3310:~/homework/lab08/eroepke$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 eroepke3.txt 2>/dev/null
Verification failure
cpre3310@cpre3310:~/homework/lab08/eroepke$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 eroepke2.txt 2>/dev/null
Verification failure
cpre3310@cpre3310:~/homework/lab08/eroepke$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 eroepke4.txt 2>/dev/null
Verified OK
cpre3310@cpre3310:~/homework/lab08/eroepke$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 eroepke5.txt 2>/dev/null
Verification failure
cpre3310@cpre3310:~/homework/lab08/eroepke$
```

5. Discussion on hash verification (10 points, 5 points each question)

- a. What is known about the message?

From these 5 text messages we gathered, we know that only one of the messages matches the original message that was used to create the signature.

- b. What is the message protected against and what is it vulnerable to?

The messages are protected against attackers being able to modify the messages from signatures as it will result in a verification failure. The messages is also protected from being able to generate a copy of private key as it can only authenticate the senders identity.

The messages is vulnerable to MITM attacks if the attacker can get access to the public key and try to trick the sender to verify a forged message

6. Discussion on what the message generated in step 8e protected against and what it is vulnerable to (compared to the message we downloaded in step 6) (10 points, 5 points each part)

The generated message is protected against unauthorized readings so only someone with the matching private key can decrypt it with the public key that decrypts the message. It is also protected against interceptions, so if an attacker does intercept the file during transfer they will not be able to decrypt since they do not have the private key.

The vulnerabilities from this is not authentication from authority in the server. We are not getting a signature so we cannot confirm the senders identity or if the message was altered. The receiver will not know if anything happened or who it came from since its not verified. Since we have no signature, an attacker can substitute its own public key and trick the sender to encrypt the message with the attacker key and the attacker can decrypt it.

In step 6, we had authenticity from authorities in the server verifying the messages was not tampered with and the identity is accurate. Step 6 overall provides integrity to who the sender and receiver is.

7. Screenshot of the signed certificate ([netid]_certificate.pem) when looked at through openssl(10 points)

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 26 (0x1a)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C = US, ST = Iowa, L = Ames, O = 3310.com, OU = homework, CN = certs.homework.3310.com, emailAddress = certs@homework.3310.com
  Validity
    Not Before: Oct 28 17:56:01 2024 GMT
    Not After : Oct 28 17:56:01 2025 GMT
  Subject: C = US, ST = Iowa, O = 3310.com, OU = homework, CN = eroepke.homework.3310.com, emailAddress = eroepke@homework.3310.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:a4:b4:99:bd:69:94:10:67:08:f8:a6:95:25:4b:
      50:66:2e:11:a0:0b:7f:a0:39:94:d7:a3:ea:ec:cb:
      4b:ce:c1:dc:e9:52:f1:fc:cd:79:23:a1:7a:4c:0e:
      c4:e4:7d:b1:ef:37:8b:3b:f1:02:16:dc:5c:cf:5d:
      a1:d7:d2:18:82:f9:0d:94:80:c0:17:4e:a8:fd:b2:
      72:9f:e6:bf:9c:83:f6:f4:73:07:7a:2e:bc:09:52:
      a8:37:3f:81:7f:3a:3d:5d:28:64:99:ac:3f:53:22:
      65:7b:7f:7d:75:7d:cf:47:06:a8:08:5e:21:06:78:
      fa:71:92:21:09:1a:e4:59:44:46:b5:a7:9c:31:91:
      1b:cb:40:c3:94:25:44:77:6f:d6:6f:8b:71:2a:fc:
      d5:ce:e1:62:0a:56:22:61:af:e8:6d:7d:68:cc:3a:
      d2:ed:51:7b:6a:3a:6b:75:e0:c3:28:a7:20:1a:52:
      c4:b9:de:c5:b5:13:b3:63:0d:a4:ad:45:9d:1f:df:
      30:ce:47:f6:3d:62:1c:55:c4:5b:11:92:40:f1:92:
      42:18:a9:c1:8f:9a:2e:77:54:11:10:f7:c6:c1:cc:
      96:f9:da:82:19:60:09:2e:34:9f:ff:c7:1f:f4:18:
      3d:ad:d6:c1:5e:01:55:94:56:39:bd:05:52:6d:10:
      70:1d
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      B5:AE:04:15:CF:53:EE:0B:1D:3F:DC:44:DA:8A:CA:64:24:B0:32:5E
    X509v3 Authority Key Identifier:
      SA:47:B0:66:5F:78:80:7C:00:09:CE:12:AF:9F:AE:23:F2:8E:65:78
  Signature Algorithm: sha256WithRSAEncryption
  Signature Value:
    e2:38:00:8d:c3:f8:d5:ee:18:87:c8:bb:57:02:17:b3:14:aa:
    c8:d5:86:c7:a5:18:14:90:21:15:f5:c1:90:29:21:82:3d:2c:
    06:d9:35:bb:00:74:87:58:61:ce:f6:7c:69:d7:e3:82:2b:07:
    73:be:37:21:34:6e:97:38:bf:fb:fb:47:46:ca:4b:5b:1b:d1:
    a0:4b:18:21:9d:d1:38:0e:22:83:56:1f:a2:7e:1e:69:5b:b4:
    ec:59:38:80:2f:3b:8d:c1:e6:4e:e6:16:40:3d:b3:92:78:7e:
    c0:50:58:a5:82:88:25:f7:3f:f3:dd:8a:9e:80:d8:48:b6:05:
    e2:d2:a3:0e:e4:f2:b9:5d:19:45:c4:2c:90:59:23:86:e2:6b:
    1a:c3:dd:11:e0:b5:e8:10:5a:8c:0e:c8:92:c4:f6:5b:8a:d5:
    43:5c:93:b8:ff:7c:26:a1:3a:d0:8c:91:93:41:1f:05:18:98:
    57:75:5c:eb:f0:de:2e:b2:40:93:cf:d9:75:5e:e0:c4:f4:e4:
    75:dd:ad:11:93:92:19:25:1d:52:1b:a9:bd:48:47:bb:20:01:
    aa:78:7b:c6:b7:18:39:f0:ff:9b:3c:75:ff:b8:80:96:92:47:
    17:48:c6:63:8a:6b:27:b6:e3:5b:5c:17:f9:29:eb:a8:77:4f:
    37:77:6a:8c
```

8. Discussion from step 12 (20 points, 10 points each answer, 10 points each why)

- a. Do any parts of the certificate match with your private key? If so, why?

None of the certificate match with my private key because the certificate only contains parts from the public key. The private key is securely stored with me and not appear in anything.

- b. What was happening during the Certificate Signing process? Why did you need to submit it for signing?

During the certificate signing process, my public key and questions I was prompted to answer was submitted to an authority on server. The authority verifies your identity which create a certificate to prove your identity. The authority also guarantees that the information has not been tampered between public and private key.

We need to submit it for signing by authority to establish trust and security. A signed certificate verifies that the public key belongs to the organization and not a forgery.